

TABLE OF CONTENTS

TABLE OF AUTHORITIES ii

 I. INTRODUCTION..... 1

 II. PROCEDURAL HISTORY..... 3

ARGUMENT 7

 I. STANDARD OF REVIEW AND BURDEN ON THE PLAINTIFF 7

 II. JURISDICTION IS LACKING AS TO DEFENDANTS VITAL AND
 DEL ROSSO 8

 III. DISMISSAL IS APPROPRIATE BASED ON THE GOVERNING
 STATUTE OF LIMITATIONS..... 12

 IV. PLAINTIFF’S COMPLAINT FAILS TO SATISFY TWOMBLY AND
 IQBAL BY RELYING ON SPECULATION, SURMISE AND
 CONJECURE AND PLEADING COGNIZABLE DAMAGES 16

CONCLUSION..... 20

TABLE OF AUTHORITIES**TABLE OF AUTHORITIES**

	Page(s)
Cases	
<i>Addison Whitney, LLC v. Cashion</i> , 2017 WL 2506604 (N.C. Super. June 9, 2017)	18
<i>Ashcroft v. Iqbal</i> , 556 U.S. 662 (2009)	7, 8, 16
<i>Assoc. Producers Ltd. v. Vanderbilt Univ.</i> , 76 F. Supp. 3d 154 (D.D.C. 2014)	12
<i>Azima v. Dechert, et al.</i> , S.D.N.Y., No. 1:22-cv-08728 (filed Oct. 13, 2022).....	6, 7
<i>Azima v. Del Rosso and Vital Management, Inc.</i> , M.D.N.C. No. 1:20-cv-00954.....	6
<i>Azima v. del Rosso</i> , No. 1:20CV954, 2021 WL 5861282 (M.D.N.C., Dec. 10, 2021)	7, 15
<i>Azima v. Rak Inv. Auth.</i> , 305 F. Supp. 3d 149 (D.D.C. 2018)	11, 12
<i>Azima v. RAK Inv. Auth.</i> , 926 F.3d 870 (D.C. Cir. 2019)	7
<i>Azima v. RAK</i> , No. 16-cv-0948 (KBJ), Dkt. No. 1 (Complaint, filed 9/30/16).....	6
<i>Bell Atl. Corp. v. Twombly</i> , 550 U.S. 544 (2007)	7, 16
<i>Boland v. Fortis Constr. Co., LLC</i> , 796 F. Supp. 2d 80 (D.D.C. 2011)	9
<i>Chloe v. Queen Bee of Beverly Hills, LLC</i> , 616 F.3d 158 (2d Cir. 2010)	9
<i>Combs v. Bakker</i> , 886 F.2d 673 (4th Cir. 1989)	9

<i>DiStefano v. Carozzi North America, Inc.</i> , 286 F.3d 81 (2001)	11
Div. 1181 Amalgamated Transit Union-N.Y. Emps. Pension Fund v. N.Y. City Dep't of Educ., 9 F.4th 91 (2d Cir. 2021).....	5
<i>Doe v. Fed. Democratic Republic of Eth.</i> , 851 F.3d 7 (D.C. Cir. 2017)	11
<i>El Omari v. Buchanan</i> , No. 20-cv-2601 (S.D.N.Y., filed March 27, 2020).....	4, 14, 15
<i>El Omari v. INTERPOL</i> , No. 211458 (2nd Cir. May 24, 2022)	3, 4, 5
<i>El Omari v. RAKFTZA, et al.</i> , No. 16-cv-3895 (S.D.N.Y.)	4
<i>Eley v. Mid/East Acceptance Corp. of N.C.</i> , 171 N.C. App. 368 (Ct. App. 2005).....	18
<i>Ennenga v. Starns</i> , 677 F.3d 766 (7th Cir. 2012)	5
<i>First Invs. Corp. v. Citizens Bank, Inc.</i> , 757 F. Supp. 687 (W.D.N.C. 1991), <i>aff'd</i> , 956 F.2d 263 (4th Cir. 1992).....	18
<i>GEM Advisors, Inc. v. Corporacion Sidenor, S.A.</i> , 667 F. Supp. 2d 308 (S.D.N.Y. 2009)	12
<i>Estate of Graham v. Morrison</i> , 168 N.C. App. 368 (2005)	17
<i>Greco v. Ulmer & Berne L.L.P.</i> , 23 Misc. 3d 875 (Sup. Ct. Kings Cty. 2009).....	10
<i>GTE New Media Servs. Inc. v. BellSouth Corp.</i> , 199 F.3d 1343 (D.C. Cir. 2000).....	9
<i>Guo Jin v. EBI, Inc.</i> , No. 05-CV-4201, 2008 WL 896192 (E.D.N.Y. Mar. 31, 2008).....	10
<i>J & J Sports Prods., Inc. v. Daley</i> , No. 06-CV-0238, 2007 WL 7135707 (E.D.N.Y. Feb. 15, 2007).....	17

<i>Kahn Lucas Lancaster, Inc. v. Lark International Ltd.</i> , 956 F. Supp. 1131 (S.D.N.Y. 1997)	10
<i>Lake Mary L.P. v. Johnston</i> , 145 N.C. App. 525 (2001)	17
<i>Leonard v. United States</i> , No. 23-CV-8571 (LTS), 2023 WL 8258263 (S.D.N.Y. Nov. 27, 2023)	17
<i>Lively v. WAFRA Inv. Advisory Grp., Inc.</i> , 6 F.4th 293 (2d Cir. 2021)	5
<i>Lupo v. JPMorgan Chase Bank, N.A.</i> , C.A. No. DKC 14-0475, 2015 WL 410273 (D. Md. Jan. 26, 2015)	9
<i>RAK Investment Authority v. Azima</i> [2020]	6
<i>Reis, Inc. v. Lennar Corp.</i> , 2016 WL 3702736 (S.D.N.Y July 5, 2016)	20
<i>Smith v. Jenkins</i> , 452 A.2d 333 (D.C. 1982).....	12
<i>Solomon v. Dechert et al.</i> , No. 22 civ. 3137, 2023 WL 6065025 (Sept. 18, 2023)	8
<i>Stratton v. Royal Bank of Can.</i> , 211 N.C. App. 78 (Ct. App. 2011).....	18
<i>Su v. Sotheby's, Inc.</i> , No. 17-CV-4577 (VEC), 2022 WL 14118016 (S.D.N.Y. Oct. 24, 2022)	16
<i>Tai Sports, Inc. v. Hall</i> , 2012 N.C.B.C. 62, ¶ 108 (N.C. Super. Ct. Dec. 28, 2012)	17
<i>Trudeau v. FTC</i> , 456 F.3d 178 (D.C. Cir. 2006)	7
<i>Van Buren v. United States</i> , 141 S. Ct. 1648 (2021)	20
<i>Wannall v. Honeywell</i> , 775 F.3d 425 (D.C. Cir. 2014)	8
<i>Whitaker v. American Telecasting, Inc.</i> , 261 F.3d 196 (2d Cir.2001).....	7, 9

White v. Consol. Plan., Inc.,
166 N.C. App. 283 (Ct. App. 2004)..... 18

Rules

Fed.R.Civ.P. 12(b) 16

Fed.R.Civ.P. 12(b)(2)..... 1

Fed.R.Civ.P. 12(b)(2)..... 7

Fed.R.Civ.P. 12(b)(6)..... 1, 3

N.Y. C.P.L.R. § 302 10

Rule 12(b)(2)..... 9

Statutes

18 U.S.C. § 1030..... 1, 12

18 U.S.C. § 1030(g) 12

Defendants Nicholas Del Rosso and Vital Management Services, LLP (“Vital”) (collectively “Defendants”) file this Memorandum in opposition to the objections to the Report and Recommendation of Magistrate Wang, recommending that pursuant to Fed.R.Civ.P. 12(b)(2) and (6), that the motion to dismiss the Complaint be granted.

I. INTRODUCTION

The present suit alleges violations of the Computer Fraud and Abuse Act (“CFAA”), 18 U.S.C. § 1030, and North Carolina law dealing with conversion. The Complaint alleges that Defendants used a computer device to hack emails from El Omari and his attorney through the use of spoofing emails. See Complaint, ¶¶ 19-21. This is Plaintiff’s fourth lawsuit alleging a conspiracy by his former employer, attorneys representing that employer, and those assisting those attorneys, to target him.

His latest claim alleges that Defendants, a North Carolina resident and his North Carolina company hacked Plaintiff, another North Carolina resident, using a computer in London. Understandably, the Magistrate found that personal jurisdiction was lacking as to Defendants since the only tenuous connection with this jurisdiction was that Defendants had been retained by a New York law firm, Defendant Dechert, and made a trip there which is not alleged to have had anything to do with any alleged hacking of Plaintiff.

But that was only one of several infirmities found by Magistrate Wang. Plaintiff acknowledged in his Complaint that the lawsuit followed others alleging a hacking scheme directed by a foreign government, one of the UAE Emirates (Ras Al

Khaimah). The Magistrate found that Plaintiff's lawsuit was barred by the statute of limitations as his claim related to a hacking incident in 2017, and he was aware of facts giving rise to his claim long before the statute of limitations expired. In fact, this case was not filed until a year and a half after one of the earlier lawsuits alleging a violation of the CFAA had been dismissed. *See* ECF 76, at 3.

The Magistrate found that the Complaint was based on speculation and conjecture. For one thing, it alleged that the hacking of his data was used in an earlier proceeding by Dechert defending its client against allegations by Plaintiff. But when it came to facts supporting that claim, the Complaint was barren of anything other than rank speculation, as the Magistrate found. *See* ECF at 17-18. Nor was there sufficient factual support for the contention that Defendants had even hacked Plaintiff. While accepting the allegations of the Complaint as true – that data relating to Plaintiff and his counsel exists on Defendants' London laptop – Plaintiff failed to offer any allegations sufficient to show that Defendants had hacked Plaintiff, and beyond that, had done so in order to obtain data to be used in defending against an earlier lawsuit by Plaintiff.

Finally, the Magistrate found that no cognizable damages had been alleged. ECF 76 at 18-19. Instead of alleging permissible damages specifically delineated under the CFAA, Plaintiff alleged vague and conclusory allegations that he as a result of the hacking he has been forced to spend sums for “legal fees and costs, and forensic computer investigation costs related to investigating, assessing the scope of the

hacking, and seeking to remedy the complete loss of the confidentiality of the emails.” Compl., ¶ 41.¹

II. PROCEDURAL HISTORY

It is difficult to tell from Plaintiff’s Objections exactly what he is challenging. Much of his discussion is directed to the failure of the Magistrate to grant his request for a temporary restraining order. See ECF 6-7. He actually filed two such emergency requests seeking. See ECF 32, 42. Incredibly, Plaintiff’s TRO applications sought to preclude compliance with an order from a court in London, directing that if any material belonging to Plaintiff exists on a laptop owned by the Vital Defendants, such material was to be removed and returned to Plaintiff’s counsel. *Id.* Plaintiff still fails to explain why this was insufficient or (twice) justified an application for emergency relief, although he seemingly includes objections to the Magistrate’s handling of his repeated TRO applications.

On June 1, 2023, Plaintiff filed his Complaint seeking damages under the CFAA and for common law conversion under North Carolina law. ECF 1. As alleged in the Complaint, Plaintiff is the former Chairman of the Ras Al Khaimah Free Trade Zone Authority, (“RAKFTZA”), a governmental entity under the authority of the Ruler of the foreign government of Ras al Khaimah, (“RAK”), an Emirate of the United Arab Emirates, (“UAE”). Compl., ¶ 4.² Plaintiff was previously convicted in the UAE of engaging in fraud. See *El Omari v. INTERPOL*, No. 211458 (2nd Cir.

¹ Defendants rely on the response to Plaintiff’s Objection filed by Dechert regarding each of these issues, including specifically the failure of Plaintiff to allege cognizable damages.

² As required under the rules governing this motion, we have assumed for purposes of this motion that the facts contained in the Complaint as true. See Fed.R.Civ.P. 12(b)(6).

May 24, 2022). The Dechert law firm previously represented RAK, including various agencies and offices. *Id.* In connection with its representation of RAK, Dechert retained Defendant Vital, which is owned by Mr. del Rosso, to provide investigative services. *Id.*

Plaintiff's claim in this case boils down to allegations that the Vital Defendants hired a firm in India (CyberRoot) to hack Plaintiff's data so that it could be used in defending lawsuits against Plaintiff, and that the hacked data could be found on a laptop in London owned by the Vital Defendants. Because those previous complaints were included in the Complaint, the Magistrate summarized them in her Report.

The first such lawsuit was filed in 2016, following the termination of Plaintiff's employment in 2012. Plaintiff sued a number of parties, including RAKFTZA. *Id.*, ¶ 17 (citing *El Omari v. RAKFTZA, et al.*, No. 16-cv-3895 (S.D.N.Y.). Plaintiff alleged, *inter alia*, breach of contract, fraud and infliction of emotional distress relating to, among other things, allegations that El Omari had been involved with Iranian sanction violations occurring in RAKFTZA. *Id.* ¶ 17. That suit was dismissed in 2017. *Id.*

On March 27, 2020, Plaintiff filed a second lawsuit against various individuals and entities associated with RAK. *Id.*, ¶ 18 (citing *El Omari v. Buchanan*, No. 20-cv-2601 (S.D.N.Y., filed March 27, 2020). This time Plaintiff alleged violations of the Civil Racketeer Influenced and Corrupt Organizations ("RICO") Act and the CFAA as well as for defamation based on what he claimed was a "continuing and organized

false smear campaign against him, including a plant of false facts in a publication by Dechert LLP and [one of its former partners] that El Omari was falsely involved in a billion-dollar fraud scheme involving his alleged employer, RAKIA.” *Id.*, ¶ 18. El Omari alleged that various individuals and entities assisting RAK violated the CFAA by sending him various spoofing emails in an attempt to discredit him. *Id.* That case was similarly dismissed at the pleading stage, in 2021. *Id.*

El Omari filed a third lawsuit, this one against the International Criminal Police Organization (“INTERPOL”), which was dismissed and affirmed on appeal. *See El Omari v. INTERPOL*, No. 211458 (2nd Cir. May 24, 2022). Plaintiff alleged that INTERPOL was liable to him for intentional infliction of emotional distress and lack of due process based on its issuance of a “red notice” stemming from his conviction for fraud in the UAE. *Id.*

Plaintiff’s claim at bar alleges that emails were hacked from his computer in 2017 by Defendants, while assisting the Dechert law firm in its representation of RAK in that prior litigation. El Omari contends that his counsel was notified in January, 2023 that a laptop in London owned by Defendants contained a tranche of emails from the account of his lawyer, Mr. Scott Moore. Complaint, ¶¶ 19-21. ³

³ Plaintiff refers to other proceedings in in his Complaint. See Compl., ¶ 19. *See, e.g.*, Div. 1181 Amalgamated Transit Union-N.Y. Emps. Pension Fund v. N.Y. City Dep’t of Educ., 9 F.4th 91, 94 (2d Cir. 2021); *Lively v. WAFRA Inv. Advisory Grp., Inc.*, 6 F.4th 293, 305 (2d Cir. 2021). The Court may take judicial notice of those other pleadings in connection with the motion to dismiss. *See, e.g.*, *Ennenga v. Starns*, 677 F.3d 766, 773–74 (7th Cir. 2012) (assessing “the statute-of-limitations defense [based on, inter alia] “judicial notice of the dates on which certain actions were taken . . . in the earlier state-court litigation — facts readily ascertainable from the public court record”).

El Omari also alleges in the Complaint that his allegations of a conspiracy to hack his data is corroborated by other lawsuits filed by third parties against various entities representing RAK. One such lawsuit relied upon by Plaintiff was filed by Farhad Azima. Complaint, ¶ 1. El Omari claims that Azima was subject to similar spoofing emails by RAK as allegedly detailed in Azima’s lawsuit. See Complaint, ¶ 19. In fact, Azima himself filed four actions against either RAK, the Dechert firm or others assisting RAK. These include a suit filed in the District of Columbia, *see See Azima v. RAK*, No. 16-cv-0948 (KBJ), Dkt. No. 1 (Complaint, filed 9/30/16); the United Kingdom, *see RAK Investment Authority v. Azima*, Counterclaim, No. HC-2016-002798, the Middle District of North Carolina, *see Azima v. Del Rosso and Vital Management, Inc.*, M.D.N.C. No. 1:20-cv-00954, filed Oct. 15, 2020, and this jurisdiction, *see Azima v. Dechert, et al.*, S.D.N.Y., No. 1:22-cv-08728 (filed Oct. 13, 2022). As for Azima, after his suit in the District of Columbia was dismissed, the High Court in the U.K. ultimately ruled that Azima had been involved in bribery and fraud. *RAK Investment Authority v. Azima* [2020] EWHC 1327 (Ch) [159, 246, 250, 381]. It also concluded that Plaintiff’s testimony was “frequently inconsistent with the contemporaneous documents,” “inherently implausible,” and at times “untruthful.” *Id.* ¶ 70–71, 127. The court also found that Azima had backdated documents to fabricate his dispute with RAKIA, and that Azima had fraudulently induced RAKIA to settle its dispute with Azima for millions of dollars; and that he conspired to misappropriate \$1,500,000 from RAKIA; committed bribery; and devised

a “sham” written agreement to “conceal that misappropriation.” [2020] EWHC 1327 (Ch), ¶¶ 93, 117, 138–42, 1891, 237, 247–50.

Azima’s lawsuit in the District of Columbia was dismissed. *See Azima v. RAK Inv. Auth.*, 926 F.3d 870 (D.C. Cir. 2019). His suit in the Middle District of North Carolina was similarly dismissed as time-barred, with the sole exception that the Court ruled that a claim based on publication of trade secrets survived the statute of limitations, which is still pending. See, e.g., *Azima v. del Rosso*, No. 1:20CV954, 2021 WL 5861282 (M.D.N.C., Dec. 10, 2021). A motion to dismiss Azima’s suit in the Southern District raising similar hacking allegations is currently pending. *See Azima v. Dechert LLP*, 1:22-cv-08728 (PGG).

ARGUMENT

I. STANDARD OF REVIEW AND BURDEN ON THE PLAINTIFF

The Plaintiff bears the burden of setting forth facts which, if true, would entitle them to the relief requested, *Ashcroft v. Iqbal*, 556 U.S. 662, 678 (2009). A complaint cannot rest on “a legal conclusion couched as a factual allegation,” nor an inference unsupported by facts. *Trudeau v. FTC*, 456 F.3d 178, 193 (D.C. Cir. 2006). Finally, speculation is insufficient to sustain the Complaint. *Bell Atl. Corp. v. Twombly*, 550 U.S. 544 (2007).⁴

Therefore, “[t]he plaintiff “bears the burden of establishing that the court has jurisdiction over the defendant when served with a Rule 12(b)(2) motion to dismiss.” *Whitaker v. American Telecasting, Inc.*, 261 F.3d 196, 208 (2d Cir.2001) (internal

⁴⁴ The Vital Defendants rely on the Memorandum submitted by Dechert in opposition to Plaintiff’s Objections to the Magistrate’s Report and Recommendation.

citations omitted), all of the essential elements of the statutory or common law causes of action are pled, and damages are proximately caused by Defendants' actions. *Iqbal*, 566 U.S. at 675-78. Plaintiff fails to satisfy that burden here. This is not a case where Plaintiff has simply relied on speculative assumptions and vague statements to show that there was a conspiracy to hack certain data and information. The Amended Complaint should be dismissed in its entirety. The facts alleged, if true, fail to aver that personal jurisdiction and venue exist, and it affirmatively shows that all claims are barred by the relevant statute of limitations governing each count.

II. JURISDICTION IS LACKING AS TO DEFENDANTS VITAL AND DEL ROSSO

Plaintiff challenges the Magistrate's conclusion that personal jurisdiction was lacking as to both Vital Defendants. It should be noted at the outset that Plaintiff fails to even address arguments by Defendants that an assertion of jurisdiction here would violate the Due Process Clause, and further, that venue is lacking. See ECF 35 at 19, 24. That alone justifies rejecting Plaintiff's objections to the Magistrate's Report inasmuch as this Court may dismiss on those grounds, even if the Magistrate acknowledge such arguments but found it unnecessary to rely on them. *See Solomon v. Dechert et al.*, No. 22 civ. 3137, 2023 WL 6065025, at * 5 (Sept. 18, 2023) (finding that Plaintiff had conceded venue was lacking by failing to address argument raised in motion to dismiss) (citing *Wannall v. Honeywell*, 775 F.3d 425, 428 (D.C. Cir. 2014) ("[I]f a party files an opposition to a motion and therein addresses only some of the movant's arguments, the court may treat the unaddressed arguments as conceded.")).

Nor is Plaintiff's objection to the Magistrate's Report sustainable regarding personal jurisdiction. "When a court's personal jurisdiction is properly challenged by a Rule 12(b)(2) motion, the jurisdictional question thus raised is one for the judge, with the burden on the plaintiff ultimately to prove the existence of a ground for jurisdiction by a preponderance of the evidence." *Combs v. Bakker*, 886 F.2d 673, 676 (4th Cir. 1989); *see also Boland v. Fortis Constr. Co., LLC*, 796 F. Supp. 2d 80, 86 (D.D.C. 2011). The same considerations and burden apply to the venue inquiry. *See Whitaker, supra*; *see also Lupo v. JPMorgan Chase Bank, N.A.*, C.A. No. DKC 14-0475, 2015 WL 410273, at *3 (D. Md. Jan. 26, 2015). Here, Plaintiff cannot meet his burden needed to sustain either personal jurisdiction or venue.

The Magistrate found that neither of the two bases alleged for asserting jurisdiction were sufficient: (1) that Defendants made trips to New York and (2) that Defendants acted as agents of Dechert, who has offices in New York and which is therefore subject to jurisdiction here. See Compl., ¶ 14. Plaintiff does not try to establish general jurisdiction, and the Magistrate concluded that Plaintiff cannot establish specific jurisdiction. "To establish personal jurisdiction over a non-resident, a court must engage in a two-part inquiry: A court must first examine whether jurisdiction is applicable under the state's long-arm statute and then determine whether a finding of jurisdiction satisfies the constitutional requirements of due process. See *Chloe v. Queen Bee of Beverly Hills, LLC*, 616 F.3d 158, 163-64 (2d Cir. 2010); *GTE New Media Servs. Inc. v. BellSouth Corp.*, 199 F.3d 1343, 1346 (D.C. Cir. 2000) (citations omitted). Plaintiff tries to argue that Defendants "transact[ed]

. . . business within the state or contract[ed] anywhere to supply goods or services in the state. . . .” See N.Y. C.P.L.R. § 302(a *inter alia*)(1).

Plaintiff argues, first, that Defendants “contracted” to supply “goods or services” within the state within the meaning of the New York long-arm statute because they were hired by Dechert, a law firm with a New York office, and Defendants delivered a secure device to New York. ECF 77 at 12. The Magistrate made short shrift of Plaintiff’s claims. As far as claims that Defendants were hired by a New York law firm, the Magistrate correctly looked to the Complaint, which alleged that they had been hired by a partner in the London Office. See 76 at 8 (citing Compl., ¶ 5).

Plaintiff engaged in the height of speculation by asserting that Defendants must have made “numerous trips to New York for personal meetings as part of his wrongful activities.” See Compl., ¶ 15. But “[c]onclusory allegations showing the presence of jurisdiction, particularly those stated only upon ‘information and belief,’ are insufficient to establish that the court has personal jurisdiction over the defendant.” *Guo Jin v. EBI, Inc.*, No. 05-CV-4201, 2008 WL 896192, at *2 (E.D.N.Y. Mar. 31, 2008). It is even more speculative to assume that if Defendants attended any meetings it was for the purpose of delivering goods or services in the state. See, e.g., *Kahn Lucas Lancaster, Inc. v. Lark International Ltd.*, 956 F. Supp. 1131, 1136 (S.D.N.Y. 1997) (holding that to establish jurisdiction in New York based on meetings in that state, the meetings must be essential to the formation or continuance of a business relationship); *Greco v. Ulmer & Berne L.L.P.*, 23 Misc. 3d

875, 889 (Sup. Ct. Kings Cty. 2009) (meetings in New York insufficient to create personal jurisdiction over Illinois law firm).

Finally, El Omari seems to suggest, without articulating any factual basis for such a theory, that the injury occurred in New York because Del Rosso delivered a device there. But that fails both factually and as a matter of law. As a factual matter, Plaintiff has no basis for alleging that the material on any device delivered to New York by Del Rosso was used in proceedings in New York by Dechert in defending against El Omari's earlier litigation. See Compl., ¶¶ 39, 58. Plaintiff makes the entirely specious argument that one can assume that because Del Rosso delivered a computer device to someone in New York, that device must have been Defendants laptop containing Plaintiff's data. But the laptop was not obtained by adversaries of Defendants in New York, as they obtained it in London. In fact, the laptop was not obtained even while in Dechert's possession.

As a matter of law, courts do not look to the place where an injury may have been felt based on the tortious conduct, but instead look to the “‘original event’ . . . ‘where the first effect of the tort ... that ultimately produced the final economic injury’ is located.” *DiStefano v. Carozzi North America, Inc.*, 286 F.3d 81, 84-85 (2001). Here, that is clearly not New York. That is particularly true of a hacking claim: courts look to where hackers are located, *see, e.g., Azima v. Rak Inv. Auth.*, 305 F. Supp. 3d 149, 171 (D.D.C. 2018) (citing *Doe v. Fed. Democratic Republic of Eth.*, 851 F.3d 7, 10 (D.C. Cir. 2017), or alternatively, the “placement of [a virus] on [the plaintiff's] computer” [which] injures the victim when he “open[s] the infected email

attachment.” *Id.* (citation omitted). Based on the latter holding, the conduct constituting the hacking only “occurs inside” the relevant jurisdiction when the attachment is opened there. *Id.* Here, no allegation is made that Plaintiff opened his computer in New York. Plaintiff alleges that the Vital Defendants – who are also located in North Carolina -- used individuals located in India to hack the computer owned by Plaintiff, who lives in North Carolina. Compl. ¶¶ 32-33.

Plaintiff notes that he alleged in the complaint that personal jurisdiction could be based on an agency relationship, see ECF 77, at 12, but fails to argue that theory in his Objections. But in order for Dechert’s role in the New York to offer personal jurisdiction as to Del Rosso and/or Vital, Dechert would have to have acted as Defendants’ agent, and done so in New York. *See Assoc. Producers Ltd. v. Vanderbilt Univ.*, 76 F. Supp. 3d 154, 166 (D.D.C. 2014) (quoting *Smith v. Jenkins*, 452 A.2d 333, 335 (D.C. 1982)). In fact, Plaintiff alleges that Defendants Vital and del Rosso were acting as agent’s of Dechert, not the other way around. That alone is fatal to any agency claim. See [*GEM Advisors, Inc. v. Corporacion Sidenor, S.A.*, 667 F. Supp. 2d 308, 318–19 \(S.D.N.Y. 2009\)](#) (cleaned up).

Accordingly, Plaintiff’s claim that jurisdiction exists lacks merit.

III. DISMISSAL IS APPROPRIATE BASED ON THE GOVERNING STATUTE OF LIMITATIONS

Both of Plaintiff’s claims are barred by the governing statute of limitations. Plaintiff’s first claim, for a violation of the CFAA, 18 U.S.C. § 1030, is governed by a two year statute of limitations. See 18 U.S.C. 1030(g). The claim alleging conversion is governed by North Carolina law, which imposes a three statutory period for filing

suit. In both cases, the relevant statutory period for bringing an action has expired. Plaintiff objects to the Magistrate's finding that the suit is time-barred.

Plaintiff does not dispute that if anyone hacked his data, it would have occurred more than three years ago. In fact, he alleges in his 2023 Complaint that his "investigation determined the hacking of an email account of El Omari occurred on or about January 12, 2017." Complaint, ¶ 20. For that reason, Plaintiff falls back on the argument that even though the intrusion into his account occurred more than three years ago, the cause of action did not accrue until 2023, after he was told that a tranche of his lawyers' emails had been found on devices belonging to Del Rosso and VMS. See Complaint, ¶ 1.

The Magistrate correctly found that the statute of limitations barred the entire lawsuit. She rejected Plaintiff's contention that he was unaware of facts triggering the statute of limitations until January, 2023, when counsel in another case notified him that Plaintiff's data had been found on Defendants' laptop. See ECF 76 at 10-12. The Magistrate noted that Plaintiff was aware, specifically, in 2017, of facts which should have alerted him to the hacking scheme since when he clicked on what turned out to be a hacking link, the screen reflected incomprehensible computer language, thereby revealing the "malicious website" which downloaded the data. ECF 76 at 5, n. 9. . See Compl., ¶ 27.

Plaintiff complains that even if he actually saw the hacking scheme unfolding before his eyes when viewing his computer screen, that was insufficient to trigger the statute of limitations because he was unaware of the significance of what he was

seeing on the screen, and beyond that, additional hacking may have occurred after that event in 2017. ECF 77 at 13-15. But even indulging in that assumption, Plaintiff ignores additional facts placing him on notice that he was being targeted. Plaintiff admits in his own complaint that more than three years before filing the instant suit, he filed an earlier lawsuit alleging a violation of the CFAA, alleging that the fraudulent use of computer systems was part of a smear campaign against him by RAK. See Complaint, ¶ 18 (referencing *El Omari v. Buchanan*, No. 20-cv-2601, filed May 4, 2020). While Plaintiff now dismisses his own allegations as being related to an earlier unrelated hack of his computer, the earlier suit by Plaintiff alleged – just as he does in this case – that RAK was responsible for hacking his systems, in violation of the CFAA. See *El Omari v. Buchanan*, D.E. 28, Ct., IV. Plaintiff alleged, specifically, that the hacking campaign alleged in that Complaint resulted in those assisting RAK being able to access his computer, and that Plaintiff suffered the same damage now alleged here, namely the loss of secrecy and confidentiality of his data. See Compl., ¶ 43 (alleging that Plaintiff “suffered the complete loss of valuable confidentiality of the data in the attorney–client communication”).

It is equally clear that a claim for conversion is time-barred. Defendant himself admits that the phishing emails allegedly used to hack his data occurred in 2016 and 2017. See Compl., ¶ 23. Plaintiff does not even try to allege any conduct constituting concealment in an effort argue that the statute of limitations governing the conversion claim was tolled. He cannot argue, as he tries to do, that he assumed that he was not being hacked since the phishing emails sought to conceal the hacking. It

defies logic to argue that Plaintiff relied on concealment of the hacking, when he filed suit seeking damages for efforts to hack his computer. See, e.g., *Azima v. de Rosso*, No. 1:20CV954 (M.D.N.C., Dec. 10, 2021), D.E. 65 at 12 (rejecting concealment claim based on the absence of any allegation that plaintiff relied on conduct by defendant intended to conceal hacking efforts).

In addition to being aware of earlier efforts to target him, specifically, Plaintiff admitted being aware that Defendants were supposedly involved in the scheme by RAK to go after or “target” those perceived as hostile to RAK. More specifically, El Omari alleged in his earlier suit that the “targeting [of] EL OMARI” on behalf of the ruler of RAK was similar to allegations filed as long ago as November 12, 2019, when Azima alleged in proceedings in the UK that RAK retained others “to ‘target’ and ‘go after’” Azima and others perceived as antagonistic to RAK. *El Omari v. Buchanan*, D.E. 28, ¶ 27. Plaintiff even alleged that Del Rosso and Vital were instrumental in that scheme, contending that they were tasked with obtaining information in August 2016, which would have been useful in connection with litigation involving RAK. *Id.*

Finally, it is no answer to say that even if the statute of limitations bars filing suit based on the 2017 hacking incident, Plaintiff is entitled to sue for the subsequent hacking of his computer. See ECF 77 at 14. But there was no allegation directed to hacking of El Omari’s computer after 2017. All that is alleged is that emails or data after 2017 was found on Defendants’ London laptop. In any event, Plaintiff himself alleged when he filed suit in March, 2020 – more than three years before filing the

instant lawsuit -- that he was aware of a “continuing” scheme by RAKIA to plant false emails on his computer. See Compl., ¶ 18.

Consequently, the entire complaint is deficient and should be dismissed.⁵ Because all three causes of action (for violation of the CFAA, conspiracy to violate the CFAA and conversion), all would be time barred, dismissal is appropriate.

IV. PLAINTIFF’S COMPLAINT FAILS TO SATISFY TWOMBLY AND IQBAL BY RELYING ON SPECULATION, SURMISE AND CONJECTURE AND PLEADING COGNIZABLE DAMAGES

This case should be dismissed, alternatively, based on the failure to comply with *Twombly* and *Iqbal*. The allegation that Defendants hacked Plaintiff’s data is, at best, based on speculation and conjecture, which cannot survive under Rule 12(b).

Plaintiff’s theory is based on allegations that (1) he received three phishing emails in 2017, ¶ 23, (2) Defendants hired and paid a firm (CyberRoot) which had been accused in a press article of hacking, ¶¶ 3, 32, 33, and (3) “a backup copy of emails containing the email address of El Omari’s . . . counsel (smm@milopc.com)” was found on a computer in London which had been stolen from Defendants. ¶ 19. Plaintiff also alleges “upon information and belief” that (1) an individual (“Jain”) supposedly gave CyberRoot targets, which included El Omari, *id.* ¶ 33, and (2) Dechert must have wanted to use the data in defending against Plaintiff’s claims. *Id.*, ¶ 15. Based on those allegations, Plaintiff theorizes that Defendants must have been

⁵ Plaintiff throws into the mix that if all else fails, he can succeed based on the theory of equitable estoppel. But Magistrate Wang correctly held that in order for an “equitable estoppel . . . to [apply to] a conversion claim, . . . a plaintiff must allege “affirmative acts of concealment” that prevented him from bringing a suit earlier. *Su v. Sotheby’s, Inc.*, No. 17-CV-4577 (VEC), 2022 WL 14118016, at *10 (S.D.N.Y. Oct. 24, 2022). As the Magistrate found no such allegations were offered by Plaintiff.

responsible for the phishing emails in 2017 and intended to obtain documents for use by Dechert in defending allegations against its client by Plaintiff.

The Magistrate correctly found that allegations made “on information and belief,” as were the allegations in this case, are entitled to less weight. See ECF 76, at 17 (citing *Leonard v. United States*, No. 23-CV-8571 (LTS), 2023 WL 8258263, at *3 (S.D.N.Y. Nov. 27, 2023) (beliefs, even strongly held, are not facts; complaint must set forth facts showing basis for information and belief)), *see also* [*J & J Sports Prods., Inc. v. Daley*, No. 06-CV-0238, 2007 WL 7135707, at *3-4 \(E.D.N.Y. Feb. 15, 2007\)](#) (“conclusory allegations based on information and belief are insufficient”).

As a preliminary matter, Plaintiff does not even set forth allegations sufficient to sustain a claim of conversion under North Carolina law. State law requires a showing that there was: “(1) the unauthorized assumption and exercise of the right of ownership; (2) over the goods or personal property; (3) of another; (4) to the exclusion of the rights of the true owner.” *Estate of Graham v. Morrison*, 168 N.C. App. 368, 371 (2005). “At its core, conversion ‘is not the acquisition of property by the wrongdoer, but a wrongful deprivation of it to the owner’” *Tai Sports, Inc. v. Hall*, 2012 N.C.B.C. 62, ¶ 108 (N.C. Super. Ct. Dec. 28, 2012) (quoting *Lake Mary L.P. v. Johnston*, 145 N.C. App. 525, 532 (2001)). There is no allegation that Plaintiff was deprived of his emails, only that Defendants was able to access them and that – unbeknownst to Plaintiff – they were no longer confidential.

Plaintiff argues that even though he was not deprived of anything on his own computer, he was unable to use the identical emails on Defendants’ London laptop

since he did not even know they existed. That argument is not only illogical, it defies the definition of conversion, which involves “(1) the unauthorized assumption and exercise of the right of ownership; (2) over the goods or personal property; (3) of another; (4) to the exclusion of the rights of the true owners.” *Eley v. Mid/East Acceptance Corp. of N.C.*, 171 N.C. App. 368, 371 (Ct. App. 2005) (cleaned up). See also *Addison Whitney, LLC v. Cashion*, 2017 WL 2506604, at *7 (N.C. Super. June 9, 2017) (citing “growing body” of North Carolina case law holding that making copies of electronically stored information does not support claim for conversion).

Plaintiff argues in the alternative that even if he was not deprived of the use of his emails, under the discovery rule, his claim did not arise until he discovered that he had been hacked. But overwhelming caselaw holds that the discovery rule has no place in a conversion claim. See *Stratton v. Royal Bank of Can.*, 211 N.C. App. 78, 83 (Ct. App. 2011) (“[T]he claim accrues, and the statute of limitations begins to run, when the unauthorized assumption and exercise of ownership occurs—not when the plaintiff discovers the conversion”); *White v. Consol. Plan., Inc.*, 166 N.C. App. 283, 310 (Ct. App. 2004)); see also *First Invs. Corp. v. Citizens Bank, Inc.*, 757 F. Supp. 687, 690 (W.D.N.C. 1991) (finding no cases holding that “the ‘discovery rule’ ... should apply to conversion actions.”), *aff’d*, 956 F.2d 263 (4th Cir. 1992).

Beyond the above failings, the Magistrate recognized that Plaintiff’s theory suffered from yet another fatal flaw: even if one were to assume that Plaintiff’s computer was hacked, he assumes without any factual allegations to support his theory, that it was Defendants who hacked his computer, and more specifically, that

they did so in 2017 or to assist Dechert in defending against Plaintiff's lawsuit. ECF 1, ¶ 2, 14. Plaintiff argues that the existence of data on Defendants' computer relating to Plaintiff or his counsel shows that it must have been sent (or directed) through the 2017 phishing emails. ECF 77 at 17. But there is nothing tying the data on Defendants' London laptop with the 2017 phishing emails.

That speculation is rendered less – not more – reliable based on evidence offered by Plaintiff that an anonymous source distributed emails to all counsel containing the same data allegedly hacked from Plaintiff's computer. See ECF 77 at 17. While Plaintiff faults the Magistrate for not considering those anonymous emails those emails only expose the extent to which Plaintiff is willing to engage in rank speculation. Without a scintilla of evidence to support his baseless claim, he now alleges that those anonymous emails must have been sent by CyberRoot. *Id.* If anything, those anonymous emails show that someone other than Defendants were in possession of Plaintiff's data, and may have been the hacker.

Finally, Plaintiff claims the Magistrate erred in finding no cognizable damages and that the allegations were “incoherent.” See ECF 76, at 19. While previously claiming various items of damage which have specifically been found non-recoverable under the CFAA, (such as legal fees or damages resulting from the loss of confidentiality of data), Plaintiff now relies on the cost of an investigation to remedy the intrusion into his computer. See ECF 77, at 17-19. But those claims are lacking even the slightest specificity. See ECF 77, at 19-20. Moreover, Plaintiff must show that he incurred expenses investigating and remedying damage to his system. See

Van Buren v. United States, 141 S. Ct. 1648, 1660 (2021) (holding CFAA inapplicable unless the conduct “impair[ed] the ‘integrity or availability’ of data, [or] otherwise harm[ed] the database system itself”). Here, it is unclear whether the investigative and other expenses claimed by Plaintiff were related to non-recoverable damages. See *Reis, Inc. v. Lennar Corp.*, 2016 WL 3702736, at *6 (S.D.N.Y. July 5, 2016) (dismissing CFAA claim where “no allegations that the investigation was for the purpose of looking into any damage to data, programs, or server system...”).

CONCLUSION

The Court should adopt the Report and Recommendation of Magistrate Wang, and dismiss the Complaint in its entirety.

Dated: March 21, 2024

Respectfully submitted,

By /s/ Samuel Rosenthal

Samuel Rosenthal, Esq.
Lisa Herbert, Esq.
Nelson Mullins Riley & Scarborough LLP
330 Madison Avenue, 27th Floor
New York, New York 10017
Tel: 212.413.9058
Fax: 646.428.2610
sam.rosenthal@nelsonmullins.com
lisa.herbert@nelsonmullins.com

*Counsel for Nicholas Del Rosso and Vital
Management*